Design Principles for Advanced Nuclear MMIS

Yeonsub Jung
KHNP CRI, 70, 1312beon-gil, Yuseong-daero, Yuseong-gu, Daejeon, 34101, Korea
**Corresponding author: ysjung62@khnp.co.kr*

1. Introduction

APR1400 nuclear power plants have been constructed in Korean and abroad. Advanced main control room has been adopted for APR1400. Core technology of MMIS is digital instrument and control. All process information is integrated to plant computers. Control logics are written and interpreted by computer rather than by relay.

There are lots of components and system in nuclear power plants. They are graded differently. Nuclear power plants require not only to separate safety system and non-safety systems, but also to restrict sending signal from non-safety system to safety system. These kinds of requirements are specified in the regulation guidelines. There are, actually too many requirements to learn and memorize while designing. The requirements look like conflicting each other at the first glance.

This paper is to review those requirements and to attempt to list minimum basic principles and to suggest example MMIS architecture complying with the principles in systematic approach. The minimum principles are useful to validate specific MMIS design and to understand MMIS.

2. Design Principles of Advanced Nuclear MMIS

2.1 Information integration of safety and non-safety.

Operating crewmembers are in charge of nuclear power plant by monitoring plant process, evaluating and controlling them. For this purpose all information in the plant shall be collected centrally and distributed plant widely.

Information comes from both sensors of systems and operator actions of human. Sensor signals are continuous, whereas human actions are momentary at specific location.

Sensor signals are categorized as safety or non-safety, whereas human actions are not categorized.

2.2 One way communication from safety to non-safety

Safety systems are designed and manufactured in high quality so that they can operate reliably even in harsh condition. Therefore safety systems are separated from non-safety so that non-safety system cannot send monitoring or control signal to safety. Note that safety system can send monitoring and control signal to non-safety system.

2.3 Protection functions to enhance functions of safety component system.

There are protection systems to support safety component system. Protection systems generate reactor trip or ESFAS signals to safety component system. Without reactor trip signal or ESFAS, operators should be busy to control lots of components manually.

2.4 Separation among channels in safety system.

Safety system shall operate properly even if single component is out of order. Therefore safety systems consist of multiple channels with interconnection as less as possible. The multiple channels are paralleled in similar architecture. Multiple channels have advantage during maintenance too.

2.5 Information integration from channels in safety system.

Like information integration from safety and non-safety, information from multiple channels shall be integrated to evaluate safety system function.

2.6 Diverse systems coping with CCF(Common Cause Failure) of safety system.

CCF might occur when the same platform is used in the safety system even though it is highly reliable. Main cause of CCF is latent software bug in the safety system. Therefore diverse systems shall be prepared for CCF. The diverse systems are allowed not to be safety graded.

2.7 Alarm processing plant widely

Even though operators monitor plant state constantly, it is known that human is not suitable for continuous monitoring. Computer is better than human in this activity. Therefore MCR shall provide alarm processing plant widely.

2.8 Alarm processing safety system widely

When plant wide alarm processing is not available, safety system wide alarm processing shall be available. Both systems, however, shall not operate simultaneously to avoid confusion such as acknowledging alarm.

2.9 Computerized procedure system

Nuclear power plant operators are required to operate nuclear power plant via procedure rather than on their own knowledge and experiences. This is nuclear specific safety culture. There are paper based procedures and computer based procedures in nuclear power plants. It is generally understood that computerized procedures go well with advanced MMIS.

2.10 Consistent man machine interface throughout all systems

Because of segmented approach while designing nuclear power plants, it is not easy for all designers to make their user interfaces consistent throughout nuclear power plant. Practical human factor program shall be established and applied while constructing nuclear power plant. Besides, human factor engineering team shall consist of multi-disciplined specialists.

3. Implementation for Design Principles

3.1 MMIS architecture

Fig.1 shows example MMIS networks complying with MMIS principles. There are several networks. Plant wide networks satisfies requirement 2.1 and 2.7. Multichannel networks satisfies requirement 2.5 and 2.8. Single channel network satisfies requirement 2.2 and 2.4.

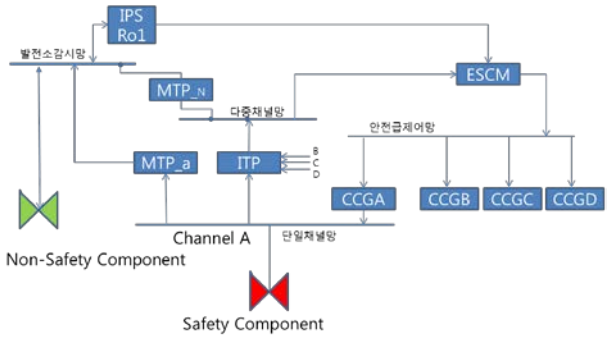

Fig.1 MMIS Architecture complying with MMIS principles

3.2 Alarm systems

Plant wide alarm processing occurs in the plant wide networks where all process information is gathered. Whereas safety widely alarm processing occurs in the multichannel networks with satisfying requirement 2.7 and 2.8

3.3 Plant Protection System

Plant protection systems are actuation systems controlling multiple safety components quickly. Actuation signals from PPS are combined in component control system which also receives manual control signals from MCR. PPS in the single channel networks meets Requirement 2.3

3.4 Diverse Protection System

Because PPS and component control systems are installed with the same platform, as might be vulnerable to common cause failure, control signal from diverse protection system or diverse manual actuation system can be injected directly to safety components. This system meeting Requirements 3.4

Diverse systems are dedicated to monitoring, controlling and automatic controlling. All these functions can be implemented separately in the several systems or collectively in a system.

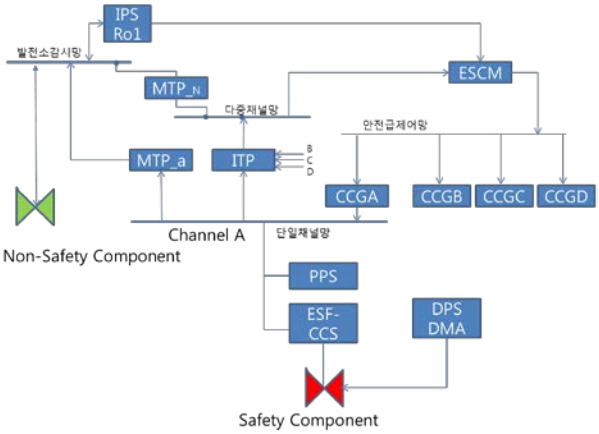

Fig.2 MMIS Architecture with detailed control layers.

3.5 Computerized Procedure

Control and monitoring system is focused on the present nuclear state rather than history of operation. On the contrary, computerized system is focused on history and on the future where operator actions shall be tracked. System with history, generally, looks complicated. Therefore computerized procedure system shall be designed ergonomically. Computerized procedure resides on the plant wide networks with meeting requirement 2.9

4. Conclusions

It takes at least 3 years for operators to understand nuclear MMIS because there are not concise basic principles established. All the requirements come from lots of regulatory documents. Furthermore, MMIS architectures complying with requirements are different from one nuclear plant to others. During construction, MMIS architecture might change to meet regulatory requirements. It is time to derive minimum basic MMIS principle in view of mathematics. Mathematics can makes all these requirements abstractive so that only quality of signal or separation between systems can be considered. This paper attempts to establish nuclear MMIS principles in view of mathematics.

The basic principles make not only MMIS design simple or reliable, but also reviewers detect deficiency in design. Without basic principles, lots of systems are added and connected and make them vulnerable during operation.

REFERENCES

[1] NRC, BTP-7-19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer based Instrumentation and Control Systems.
[2] IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations.